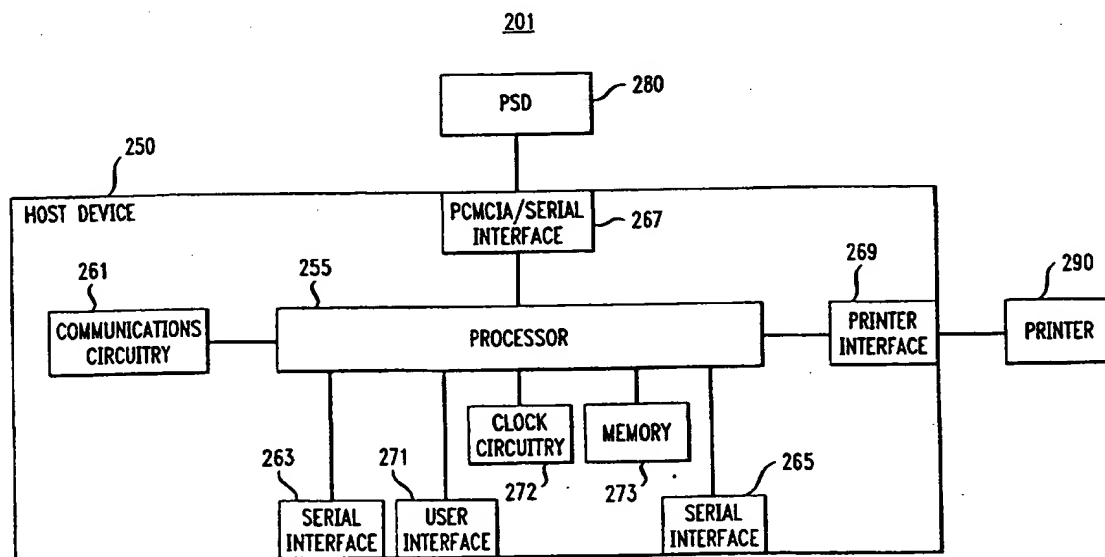




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07B		A2	(11) International Publication Number: WO 99/16023
			(43) International Publication Date: 1 April 1999 (01.04.99)
(21) International Application Number: PCT/US98/19652		(81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 21 September 1998 (21.09.98)			
(30) Priority Data: 60/059,486 22 September 1997 (22.09.97) US		Published Without international search report and to be republished upon receipt of that report.	
(71) Applicant (for all designated States except US): ASCOM HASLER MAILING SYSTEMS, INC. [US/US]; 19 Forest Parkway, P.O. Box 858, Shelton, CT 06484-0904 (US).			
(72) Inventors; and (75) Inventors/Applicants (for US only): SCHWARTZ, Robert, G. [US/US]; 191 Linden Avenue, Branford, CT 06405 (US). BROOKNER, George, M. [US/US]; 11 Surrey Drive, Norwalk, CT 06851 (US). NACLERIO, Edward [US/US]; 49 Scenic Road, Madison, CT 06443 (US). ZUIDEMA, Eric [US/US]; 4 Kendall Court, Norwalk, CT 06850 (US).			
(74) Agent: YIP, Alex, L.; Attorney at law, P.O. Box 670425, Flushing, NY 11367 (US).			

(54) Title: TECHNIQUE FOR EFFECTIVELY GENERATING MULTI-DIMENSIONAL SYMBOLS REPRESENTING POSTAL INFORMATION



(57) Abstract

In a mailing system for franking a postage indicium serving as a proof of postage, postal data including the postage needs to be communicated through such an indicium. Illustratively, the postal data is categorized into (a) invariable postal data, e.g., a device ID identifying the mailing system, which is unaffected by a franking transaction, and (b) variable postal data, e.g., the postage, which may change from one franking transaction to another. To avoid latency of the franking operation, the invariable postal data is preset for initial printing of the postage indicium, and the variable postal data is determined and set for printing in real time. In printing the postage indicium, the invariable postal data and the variable postal data are presented in that order in one or more symbols.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

-1-

DescriptionTechnique for Effectively Generating
Multi-Dimensional Symbols Representing Postal InformationTechnical Field

The invention relates to a technique for generating multi-dimensional symbols representative of information, and more particularly to a technique for
5 franking postage indicia incorporating such symbols representative of postal information.

Background of the Invention

Communications of information, e.g., via email, telephone, mail, etc., are essential in daily life.
10 Security and accuracy of such communications invariably are the major concerns.

To prevent tampering or unauthorized use of communications containing vital information, cryptographic methodologies for maintaining secrecy of
15 data communications have been developed. One such methodology is RSA cryptographic method, named after its developers, Rivest, Shamir and Adleman. For details on the RSA method, one may refer to: R. Rivest et al., "A Method for Obtaining Digital Signatures and Public Key
20 Cryptosystems," Communications of the ACM, Vol. 21, No. 2, February 1978. The RSA method involves a public key algorithm which uses a private key for encryption of data and a public key for decryption thereof. Unlike a
25 private key, a public key can be published and made known to the public. The keys for the RSA algorithm are generated mathematically, and are computational inverses to each other. The success of the RSA method depends on the use of very large numbers for the keys.

In addition to providing data encryption, some
30 cryptographic methods can be used to authenticate a message. For example, public key algorithms such as the

-2-

aforementioned RSA algorithm can be used to generate a "digital signature" for verifying the origin of the message and the identity of the sender. Another algorithm known as the "Digital Signature Algorithm (DSA)" can be used for that purpose as well. For details on the DSA, one may refer to: "Digital Signature Standard (DSS)," FIPS PUB 186, May 19, 1994. A digital signature is distinct for each message. The sender of the message uses his/her private key to digitally sign the message, and the resulting digital signature accompanies the message. The recipient of the message uses the sender's public key to verify the digital signature. If any alteration in either the signature or message occurs, the signature does not verify.

Information may be represented using a symbology. One such symbology comprises barcodes which may be one-dimensional or two-dimensional (2-D), and may be optically scanned to recover the information represented thereby. A 2-D barcode may be formatted in accordance with the well-known Uniform Symbology Specification PDF 417. Another symbology comprises data matrix symbols, which are formatted in accordance with the "International Symbology Specification - Data Matrix," AIM International Technical Specification, AIM International, Inc., 1996 (hereinafter the "Data Matrix specification"), and may also be optically scanned to recover the information represented thereby.

As is well known, a data matrix symbol is made up of square modules or cells representing information. Figs. 1A and 1B illustrate one such data matrix symbol (denoted 100), and its finder patterns (collectively denoted 150) defining data regions in symbol 100, respectively. As jointly shown in Figs. 1A and 1B, data matrix symbol 100 includes data regions I, II, III and IV containing square modules which are disposed in arrays. A dark module represents a first data value (e.g., binary bit "1"), and a light module represents a second data

-3-

value (e.g., binary bit "0"). Symbol 100 is typically square in shape, and the number of rows (or number of columns) of the modules, and thus its size, increases with the amount of data represented thereby. Symbol 100 also includes codewords for checking and correcting errors in the data after its communication, thereby affording accuracy of the communicated data. For example, symbol 100 is of the type of the so-called "error checking and correcting (ECC) 200" data matrix symbol, and the codewords therein are generated in accordance with the well-known Reed-Solomon error correction technique.

Each data region in symbol 100 is surrounded by a finder pattern which is one module wide. For example, the finder pattern for data region I consists of solid arrays 153 and 155 made up of dark modules only, and broken arrays 157 and 159 made up of alternating dark and light modules; the finder pattern for data region II consists of solid arrays 163 and 165, and broken arrays 167 and 169; and so on and so forth. In a well known manner, the finder patterns of a data matrix symbol determine, among other things, physical size and distortion of the symbol.

Because of the ubiquitous presence of computers, in particular, personal computers (PCs), it is anticipated that use of a general purpose computer, in lieu of a specialized postage meter, to frank or print postage indicia serving as a proof of postage on mailpieces is imminent. To deter printing of unauthorized postage, the postage indicium applied on a mailpiece includes postal information which is digitally signed, and thereby can be authenticated by a postal authority when the mailpiece is processed. To facilitate the mail processing, the indicium includes a machine readable portion including a 2-D symbol, e.g., a 2-D barcode, readable by an optical scanner.

Summary of the Invention

In accordance with the invention, the postage indicium is generated in a pipeline fashion to expedite a postage franking transaction. For example, in generating the postage indicium which includes at least one symbol, e.g., a data matrix symbol, representing postal data elements, as soon as new information concerning a bit map for the print image of the symbol is made available, such information is utilized to print the symbol as much as possible. To facilitate the pipeline operation, the layout of the bit map is designed in such a way that the leading portion of the bit map corresponds to those postal data elements which can be determined without regard to any subsequent postal data elements, which correspond to the remaining part of the bit map. To that end, the postal data elements to be represented are arranged in such an order that those postal data elements (e.g., postal data elements concerning accounting of dispensed postage) which need to be determined based on other postal data elements (e.g., current dispensed postage) are disposed after such other postal data elements in the bit map representation, thereby obviating the need to modify the bit map as it is being laid out and made available for printing.

In accordance with an aspect of the invention, the postal data elements are categorized into invariable and variable postal data elements. The invariable postal data elements are those data elements which are unaffected by the postage franking transaction while the remaining variable postal data elements are subject to change during the transaction. In particular, the invention embraces the approach where a single symbol is used in the machine readable portion to represent a combination of the invariable and variable postal data elements, with the invariable postal data elements processed first and represented by the leading portion of the symbol, followed by the variable postal data elements

represented by the remaining portion of the same symbol, as the invariable postal data elements are independent of the subsequent, variable postal data elements.

The invention also embraces a multi-symbol approach where the machine readable portion includes at least a first symbol and a second symbol. The first symbol is used to represent those invariable postal data elements and preset for printing. The second symbol is used to represent the variable postal data elements and created in real time of the franking transaction. During the franking transaction, to avoid latency, the first symbol is printed before the second symbol.

To further expedite the postage franking transaction, prior to the transaction, selected data (e.g., the postage to be dispensed) having an unknown value is assumed using a predicted value to generate one or more candidates for at least one postal data element dependent upon the selected data. The predicted value may be statistically determined. The actual value of the selected data is subsequently compared with the predicted value. If the actual value matches the predicted value, the candidate corresponding to the predicted value is adopted during the transaction.

Other ways to expedite the franking transaction include computing at least part of a digital signature for authenticating the postal data elements represented by the postage indicium prior to the franking transaction. Where the size of a symbol in the machine readable portion of the postage indicium exceeds the print coverage of a single printhead in a printer, a print assembly in accordance with the invention which includes multiple printheads is used to print the symbol or its equivalent, thereby effectively communicating the data represented by the symbol in a single pass of the print assembly, as opposed to multiple passes required of the single printhead.

Brief Description of the Drawing

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying drawing, in which:

Figs. 1A and 1B illustrate a prior art data matrix symbol and its finder patterns, respectively;

Fig. 2 is a block diagram of a mailing system in accordance with the invention;

Fig. 3 is a block diagram of a postal security device used in the mailing system of Fig. 1;

Fig. 4 illustrates a postage indicium generated by the mailing system of Fig. 1;

Fig. 5A is a flow chart depicting a subroutine for generating a part of the postage indicium of Fig. 4;

Figs. 5B and 5C are flow charts jointly depicting a main routine for generating the postage indicium of Fig. 4;

Fig. 6 illustrates a segmented data matrix symbol in accordance with the invention;

Fig. 7 illustrates a printhead assembly for generating the symbol of Fig. 6; and

Fig. 8 illustrates a second, segmented data matrix symbol in accordance with the invention.

Throughout the figures of the drawing, the same reference numerals and characters are used to denote like features, elements, components or portions of the illustrated system.

Detailed Description

Fig. 2 illustrates mailing system 201 embodying the principles of the invention for franking postage onto a given medium, e.g., a mailpiece, tape, etc. As shown in Fig. 2, system 201 includes host device 250, postal security device (PSD) 280 and printer 290. System 201 may be configured as an "open system," where host device 250 comprises a personal computer (PC), workstation or

-7-

general purpose computing machine, and PSD 280 and printer 290 serve as peripherals to host device 250. System 201 may alternatively be configured as a "closed system," where host device 250 and printer 290 are
5 dedicated to the postage franking operation and typically enclosed in the same casing, and where PSD 280 may or may not be enclosed therein.

Without loss of generality, in this illustrative embodiment, system 201 is configured as a
10 closed system. Central to host device 250 is processor 255 which is programmed to, among other things, communicate and process data to effect postage franking in accordance with the invention. Device 250 is connected through printer interface 269 to printer 290
15 for controllably printing postage indicia onto a given medium, which serve as a proof of postage. Printer 290 may incorporate well known laser, thermo transfer or inkjet technology. Device 250 also includes communications circuitry 261, serial interfaces 263 and
20 265, PCMCIA or serial (PCMCIA/serial) interface 267, user interface 271, clock circuitry 272 and memory 273. Communications circuitry 261 includes conventional modem circuitry for establishing connections to communication networks, e.g., the Internet. Serial interfaces 263 and
25 265 may be used for connection with devices such as a conventional optical scanner and postage scale. Interface 267 in this instance is used for connection with PSD 280 which is realized as an integrated circuit (IC) card or a "smart" module peripheral to device 250,
30 and user interface 271 for connection with a keypad (not shown), a display (not shown) and/or an indicator device such as a mouse (not shown) for user inputs. Clock circuitry 272 keeps track of the current date and time for system 201. Memory 273 is used to store data and
35 program routines for instructing processor 255 to perform various functions. One such program routine may be a postage franking routine described below for instructing

processor 255 to carry out the postage franking operation in accordance with the invention.

Referring to Fig. 3, PSD 280 includes PCMCIA and/or serial (PCMCIA/serial) interface 301 for
5 interfacing with and insertion into host device 250, cryptographic processor 305, and secure memory 307. The components in PSD 280 may be realized using a chip set of the type of the NETARMOR VMS310 chip set manufactured by VLSI Technology, Inc, or alternatively the chip set
10 typified by smart card technology.

Secure memory 307 which is a nonvolatile memory includes a descending register and an ascending register. In a conventional manner, the descending register is used to keep track of an amount of postage available for
15 dispensation. On the other hand, the ascending register is used to keep track of an amount of postage dispensed. When the value of the descending register decreases over time below a predetermined limit, system 201 can no longer dispense postage until the descending register is
20 reset. Such a reset may be achieved by way of electronic funds transfer via a dial-up connection with a computerized central facility using communications circuitry 261, in accordance with a well-known telemeter setting (TMS) technique.

25 In this particular illustrative embodiment, secure memory 307 also includes a well known digital signature algorithm (DSA), a private key and the corresponding public key in accordance with the DSA. The public key may be made available to the public in a PSD
30 certificate. For instance, using the DSA, cryptographic processor 305 may sign specified postal data with the private key to generate a digital signature to be included in a postage indicium. The PSD certificate containing the public key may also be provided in the
35 indicium for the postal authority to verify the digital signature to authenticate the postage indicium.

Fig. 4 illustrates postage indicium 400 which serves as a proof of postage and is generated by system 201 in accordance with the invention. Indicium 400 includes human readable portion 405 and machine readable portion 410. Portion 405 may include information concerning the date of mailing, postage, device ID, origination town and zip code, mail class, etc. Machine readable portion 410 may include one or more symbols representing the postal data required by the postal authority, and the digital signature for authenticating the indicium as mentioned before. In this particular illustrative embodiment, portion 410 includes multiple symbols, e.g., data matrix symbols 415 and 420 in accordance with the well known Data Matrix specification, which jointly represent the required postal data. Such postal data, for example, includes the device ID which identifies system 201, ascending register value, postage, digital signature, date of mailing, originating address licensing zip code, software ID which identifies application software including the aforementioned postage franking routine in system 201, descending register value, PSD certificate, mail class (or rate category), etc.

To expedite each postage franking transaction especially where system 201 needs to handle a high volume of mailpieces, the machine readable portion of a postage indicium which includes at least one symbol is printed in a pipeline fashion in accordance with the invention. That is, in printing the symbol, as soon as new information concerning a bit map for the print image of the symbol is made available, printer 290 utilizes such information to realize the symbol as much as possible. To facilitate the pipeline operation, the layout of the bit map is designed in such a way that the leading portion of the bit map corresponds to those postal data which can be determined without regard to any subsequent postal data, which correspond to the remaining part of

the bit map. To that end, processor 255 arranges the postal data to be represented in such an order that those postal data (e.g., the ascending and descending register values) which need to be determined based on other postal data (e.g., the postage) are disposed after such other postal data in the bit map representation, thereby obviating the need to modify the bit map as it is being laid out and made available to printer 290 for printing.

We have recognized that of the required postal data, some data elements such as the device ID, originating address licensing zip code, software ID and PSD certificate are invariable with respect to system 201, and some other data elements such as the date of mailing are invariable over a period of time, e.g., 24 hours, and the remaining data elements such as the ascending register value, postage, descending register value and mail class may vary from one franking transaction to another.

Thus, in particular, the invention embraces the approach where a single symbol may be used in the machine readable portion to represent a combination of invariable and variable postal data elements, with the invariable postal data elements processed first and represented by the leading portion of the symbol, followed by the variable postal data elements represented by the remaining portion of the same symbol, as the invariable postal data elements are independent of the subsequent, variable postal data elements.

The invention also embraces a multi-symbol approach where as illustrated in Fig. 4, machine readable portion 410 includes at least two symbols, e.g., data matrix symbols 415 and 420. One of the symbols may represent only those invariable postal data elements. Such a symbol is "invariable" or "fixed" by virtue of the invariable postal data elements represented thereby, and thus can be preset for printing in each franking transaction. The other "variable" symbol may represent

-11-

the remaining postal data elements which may vary from transaction to transaction.

However, in this particular illustrative embodiment, data matrix symbol 415 represents those postal data elements which are invariable over at least a period of time. For example, in addition to the invariable postal data elements such as the device ID, originating address licensing zip code, software ID and PSD certificate, data matrix symbol 415 also represents the date of mailing which changes daily. Notwithstanding such, symbol 415 needs to be created only once per day with the current mailing date and is then set in a print memory for printing in each franking transaction for the rest of the day. Thus, the creation of symbol 415 does not consume real time during the franking transaction. On the other hand, the creation of symbol 420 representing the remaining postal data elements which may vary from transaction to transaction consumes real time.

Similarly, human readable portion 405 can be divided into two parts, namely, a "fixed" part including, e.g., information concerning the origination town and zip code, device ID and date of mailing which is invariable over at least a period of time; and a "variable" part including, e.g., information concerning the postage and mail class which may vary from transaction to transaction. The fixed part may be preset in the print memory for printing, and the variable part may be created in real time when the transaction occurs.

We have recognized certain advantages of the multi-symbol approach over the aforementioned single symbol approach. As mentioned before, each data matrix symbol includes error correction codewords to help ensure scanning success of the communication of the data represented thereby. In the multi-symbol approach, the computation of the error correction codewords for symbol 415 representing invariable postal data elements is completed prior to the franking transaction and does not

consume real time of the transaction. However, the computation of the error correction codewords for symbol 420, which represents variable postal data elements and is created during the franking transaction, consumes real
5 time. So does the computation of the error correction codewords for a single symbol representing both variable and invariable postal data elements in the single symbol approach. Nevertheless, the computation of the codewords for symbol 420 in the multi-symbol approach is simpler as
10 the codewords afford error protection to fewer data elements than that for a single symbol in the single symbol approach. As a result, the multi-symbol approach is more real-time efficient in computing error correction codewords.

15 Other advantages of the multi-symbol approach over the single symbol approach include the versatile adaptability of multiple symbols into the required space of machine readable portion 410. For example, data matrix symbols 415 and 420 occupy relatively small square
20 spaces, respectively, with respect to the otherwise, single symbol occupying a relatively large square space. Because of the smaller sizes of symbols 415 and 420, they can readily fit into the required space, e.g., a limited rectangular space. In addition, because of the
25 availability of the few predetermined sizes of a data matrix symbol corresponding to the maximum amounts of data represented by the symbol, a single symbol may assume a data matrix symbol having much unused data capacity, thus wasting much space, and yet because of its
30 postal data amount needed to be represented, the single symbol may not assume a smaller size. However, symbols 415 and 420 may assume data matrix symbols of different sizes to maximize use of the data capacities afforded thereby, and to save space at the same time.

35 Regardless of whether a single symbol or multiple symbols are used to represent the required postal data elements, because of the manipulation of the

-13-

order of the postal data elements, e.g., invariable postal data elements followed by the variable postal data elements, in accordance with the invention, the sequence of the postal data elements represented by the single
5 symbol or multiple symbols when read may not match the sequence expected by the postal authority. If that is the case, each postal data element represented by the single symbol or multiple symbols may be preceded by a field identifier indicating the order of the data element
10 with respect to the sequence expected by the postal authority.

Figs. 5A, 5B and 5C illustrate the aforementioned postage franking routine in accordance with the invention. This routine includes (a) subroutine
15 503 in Fig. 5A for generating fixed data matrix symbol 415 and the fixed part of human readable portion 405, representative of those postal data elements which are unaffected by franking transactions, and (b) main routine 550 in Figs. 5B and 5C for franking postage indicium 400,
20 including generating variable data matrix symbol 420 and the variable part of human readable portion 405, representative of the remaining postal data elements which may vary from one franking transaction to another.

Instructed by subroutine 503 in Fig. 5A,
25 processor 255 in system 201 detects any interrupt concerning a change in the date of mailing which is a required postal data element for postage indicium 400, as indicated at step 513. Such an interrupt may be automatically generated by clock circuitry 272 at the
30 beginning of each day, or caused by other date change mechanisms or by a user input adjusting the mailing date through user interface 271. When such an interrupt is detected, processor 255 at step 516 assembles the data concerning the new mailing date and other invariable
35 postal data elements corresponding to fixed data matrix symbol 415 which are pre-stored in memory 273. At step 519, processor 255 computes the error correction

codewords for the assembled data in accordance with a well known error correction technique, e.g., the Reed-Solomon error correction technique. Processor 255 at step 521 then prepares a bit map for a print image of fixed symbol 415 representing the assembled data and error correction codewords just computed which are arranged in accordance with the Data Matrix specification. Processor 255 stores such a bit map in a print memory which may be a part of memory 273, as indicated at step 523. In addition, processor 255 at step 527 assembles data concerning the new mailing date and those invariable postal data elements corresponding to the fixed part of human readable portion 405. At step 530, processor 255 prepares a second bit map for a print image of the fixed human readable part based on the assembled data. Processor 255 at step 533 stores the second bit map in the print memory as well. Thus, during a franking transaction, printer 290 can readily retrieve from the print memory the preset bit maps for printing data matrix symbol 415, and the fixed part of human readable portion 405.

In order to fully appreciate main routine 550 involving creation of variable data matrix symbol 420, the generation of the aforementioned digital signature which is also represented by symbol 420 will now be described. In this illustrative embodiment, the required postal data elements represented by machine readable portion 410 are signed in accordance with a well known cryptographic algorithm, e.g., the DSA. The resulting digital signature whose representation is included in symbol 420 is used for authentication of postage indicium 400.

The digital signature is composed of a first signature value "r" which is 20 bytes long, and a second signature value "s" which is also 20 bytes long. In accordance with the DSA, the generation of the signature value "r" involves generation of a random (or psuedo-

-15-

random) integer "k" in each franking transaction. The value "r" is a function of the integer "k" and certain given DSA parameters, and independent of the postal data elements to be signed. However, the generation of the signature value "s" involves applying a secure hash algorithm (SHA) onto the postal data elements to be signed. One such SHA is described in "Secure Hash Standard," FIPS PUB 180-1, April 17, 1998. Specifically, the signature value "s", dependent on the values of the postal data elements to be signed, may be expressed as follows:

$$s = (k^{-1}(\text{SHA}(M) + xr)) \bmod q, \quad [1]$$

where " k^{-1} " represents the multiplicative inverse of the random integer k; "M" represents the postal data elements to be signed onto which the SHA is applied; "x" represents the value of the aforementioned private key stored in secure memory 307; "r" represents the aforementioned first signature value; and "mod q" represents a standard modulus operation having a base q, which is one of the given DSA parameters.

Referring to Fig. 5B, instructed by main routine 550, processor 255 for each franking transaction causes cryptographic processor 305 in PSD 280 to generate a random integer k, as indicated at step 553. Based on the value of k, processor 305 at step 557 computes the first signature value r which is independent of the values of the postal data elements to be signed, i.e., M in expression [1]. In accordance with an aspect of the invention, processor 305 at step 561 computes $\text{temp1} = k^{-1}$ and $\text{temp2} = xr$ in expression [1] even before knowing the actual mail class and postage to be dispensed which, however, affects only M, and thus $\text{SHA}(M)$, thereby gaining some time to compute the second signature value s before such actual mail class and postage become known.

In accordance with another aspect of the invention, processor 305 further pre-computes candidates

-16-

of the second signature value *s* based on one or more predicted mail classes and postage values to be dispensed, as indicated at step 564. Such predicted mail classes and postage values are formed in pairs based on statistics concerning past usage of mail classes and postage. In this example, system 201 uses three predicted mail class/postage pairs, which are the last mail class and postage actually dispensed by system 201, and the two most statistically likely mail class/postage pairs, e.g., first class mail/32¢ and first class mail/55¢, where 32¢ and 55¢ correspond to the two lowest weight limits of the first class mail. Once the unknown mail class and postage to be dispensed is assumed to be a prediction thereof, all of the variable postal data elements including the postage, ascending register value, descending register value and mail class are defined. Accordingly, *M* in expression [1], which represents all of the required postal data elements represented by machine readable portion 410, including the variable postal data elements, is also defined. In this instance, processor 305 pre-computes three "*s*" candidates corresponding to the respective predictions in accordance with expression [1].

As soon as processor 255 detects the actual mail class and postage entry by a user through user interface 271, processor 255 determines whether the actual postage and mail class just entered match any of the predictions, as indicated at step 566. If it is determined that the mail class and postage entry matches one of the predictions, processor 255 causes processor 305 to select the "*s*" candidate corresponding to the matched prediction for use as the actual second signature value, as indicated at step 569, thereby expediting the postage franking transaction. Otherwise, if it is determined that the mail class and postage entry does not match any prediction, processor 255 causes processor 305 to compute the actual second signature value based on the

-17-

mail class and postage entry, and the pre-computed temp1 and temp2 above, in accordance with expression [1], as indicated at step 571.

As previously mentioned, the franking operation is performed by system 201 pursuant to the inventive pipeline approach. With the bit map of fixed symbol 415 preset in the print memory as described before, as soon as processor 255 detects a signal (e.g., from a conventional mail feeder (not shown) connected to system 201, or user interface 271) requesting printing of a postage indicium, say, indicium 400, corresponding to the aforementioned mail class and postage entry, processor 255 causes printer 290 to start printing fixed symbol 415 advantageously without latency, as indicated at step 572.

While symbol 415 is being printed, processor 255 is creating variable symbol 420 and the variable part of human readable portion 405, taking advantage of the print time for symbol 415. Specifically, referring to Fig. 5C, processor 255 at step 573 causes cryptographic processor 305 to provide thereto (a) the ascending register value and (b) the descending register value, taking into account the current dispensed postage, and (c) the digital signature which is composed of the aforementioned first signature value from step 557 and second signature value from step 569 or step 571. At step 576, processor 255 computes error correction codewords for the digital signature and the variable postal data elements including the postage, mail class, and ascending and descending register values received by processor 255, in accordance with a well known error correction technique, e.g., the Reed-Solomon error correction technique. At step 579, processor 255 prepares a bit map for a print image of variable symbol 420 representing such digital signature, variable postal data elements and error correction codewords which are arranged in accordance with the Data Matrix

-18-

specification. At step 581, processor 255 transfers the resulting bit map to the print memory.

In addition, processor 255 at step 583 prepares another bit map for a print image of the variable part of human readable portion 405 including the dispensed postage and mail class. At step 585, processor 255 transfers the resulting bit map to the print memory as well. As soon as fixed symbol 415 is printed, at step 587, processor 255 causes printer 290 to start printing symbol 420, followed by human readable portion 405, based on the respective bit maps in the print memory, thereby realizing postage indicium 400.

As mentioned before, the use of additional data matrix symbols to represent the same amount of data enables one to reduce the size of individual symbols. However, in the event that the number of symbols used is limited, and the size of at least one of the symbols is larger than the print coverage of a printhead (not shown) of printer 290, the oversize symbol cannot be printed in a single pass of the printhead, incurring at least a second pass thereof to complete the oversize symbol. Such multiple passes of the printhead, versus a single pass thereof, to realize machine readable portion 410 undesirably reduce significantly the speed of the postage franking operation.

Referring back to Figs. 1A and 1B, as described before, a data matrix symbol, e.g., data matrix symbol 100, includes four finder patterns (collectively denoted 150) for data regions I, II, III and IV, respectively. We have recognized that if data matrix symbol 100 is oversize and needs to be divided into segments for printing in a manner described below, an innocuous way to divide it is to separate data regions I and II from regions III and IV by solid arrays 155 and 165 of the finder patterns for data regions I and II, respectively. Fig. 6 illustrates the resulting segmented data matrix symbol, denoted 600. As shown in Fig. 6, symbol 600

includes upper symbol segment 610 and lower symbol segment 620. Except for solid arrays 155 and 165 which no longer appear in symbol 600 and are replaced by an inter-segment gap having a width G, which is exaggerated for illustrative purposes, symbol 100 is identical to symbol 600. In any event, the missing solid arrays 155 and 165 from symbol 100 are inconsequential to the determination of the size and distortion of symbol 100 using the remaining finder patterns. Thus, for data communications, symbol 600, even with its inter-segment gap narrower than G, is equivalent to symbol 100.

In accordance with the invention, in printing an oversize data matrix symbol, a printhead assembly comprising multiple printheads is used to print the symbol in a single pass of the assembly to maintain the high efficiency of the postage franking operation. Fig. 7 illustrates printhead assembly 700 in accordance with the invention which includes printheads 703 and 705, which are connected and arranged (or ganged) close to each other in the assembly. As shown in Fig. 7, the leading edge 711 of printhead 703 is aligned with the leading edge 713 of printhead 705. Assembly 700 is controlled by printer 290 to print in direction A to realize an oversize data matrix symbol, say, symbol 100, where the length of the symbol is longer than each of the length y1 of the print coverage by printhead 703 and the length y2 of the print coverage by printhead 705.

In practice, in assembly 700 printhead 703 is inevitably separated from printhead 705 by a separation. Without sacrificing the data integrity of oversize symbol 100, in accordance with the invention, assembly 700 generates a version of symbol 600, instead, which is equivalent to symbol 100. Specifically, printhead 703 controllably prints symbol segment 610 while printhead 705 controllably prints symbol segment 620, with the width of the otherwise solid arrays 155 and 165 provides the tolerance for the separation between printheads 703

and 705. In other words, the separation between printheads 703 and 705 is made to fall within gap G in Fig. 6, and is denoted G', which is also exaggerated in Fig. 7. In effect, gap G is provided to compensate for mechanical tolerance and the alignment of printheads 703 and 705.

It should be noted at this point that in accordance with the Data Matrix specification, each data matrix symbol can be realized in either a "dark on light" format or a "light on dark" format, representing identical information including the finder patterns. For example, symbol 100 is illustrated in Fig. 1 in a "dark on light" format. Its "light on dark" counterpart has each light module in symbol 100 become a dark module and conversely each dark module become a light module. In particular, the solid arrays in the "light on dark" counterpart consists of light modules or blanks. As such, print assembly 700 is particularly advantageous to realize data matrix symbols in the "light on dark" format, with the separation G' between printheads 703 and 705 effectuating the solid arrays therein which are naturally blank.

Similarly, printhead assembly 700 may also be used to print an oversize human readable portion, although the data integrity there is much less susceptible to any misalignment of printheads 703 and 705 in the assembly.

Fig. 8 illustrates another segmented data matrix symbol 800 equivalent to oversize symbol 100. Symbol 800 is designed for those printers which print in direction B, as opposed to direction A in Fig. 7. Similarly, the printhead assembly (not shown) for generating a version of symbol 800 includes first and second printheads separated from each other by a separation G'. The first printhead controllably prints symbol segment 810 and the second printhead controllably prints symbol segment 820, with the separation G' falling

within gap G (also exaggerated for illustrative purposes) of symbol 800, where gap G coincides with the otherwise solid arrays of oversize symbol 100.

5 The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various modifications or alterations which, although different from the exemplary embodiments described herein, are within the scope as defined by the appended claims.

10 For example, in the disclosed embodiment, data matrix symbols are used to illustrate the principles of the invention. However, it will be appreciated that other barcodes such as PDF 417 barcodes, or other similar segmenting image presentations, stacked codes or symbols
15 representative of information may be used, instead, to implement the invention.

In addition, in the disclosed embodiment, the bit map for a print image representing data is illustratively generated in host device 250. However, it
20 will be appreciated that alternatively the data will be provided by device 250 in the form of image vectors to printer 290, in accordance with a printer protocol or printer control language. Printer 290 will then generate the bit map based on the received image vectors.

25 Moreover, in the disclosed embodiment, machine readable portion 410 illustratively includes multiple symbols which are readable by a scanner. It will be appreciated that in accord with the invention, the multiple symbols as a whole will be scanned only once by
30 the scanner, and the presence of the multiple symbols will be recognized by the single pass of the scan. The scanner will then decode each individual symbol to recover the postal information represented thereby.

35 Finally, the illustrative embodiment of the invention is disclosed herein in a form in which the various data processing functions are performed by discrete functional blocks. These functional blocks may

be implemented in various ways and combinations using logic circuitry and/or appropriately programmed processors, as will be known to those skilled in the art.

-23-

Claims

1. Apparatus for processing a plurality of postal data elements, a first one of the plurality of postal data elements being a function of at least a
5 second one of the plurality of postal data elements, the apparatus comprising:

a processor for arranging the plurality of postal data elements in an order where the second postal data element precedes the first postal data element; and

10 an output for providing a representation representing the plurality of postal data elements in the arranged order.

2. The apparatus of claim 1 wherein the representation includes at least one barcode.

15 3. The apparatus of claim 2 wherein the barcode is a 2-dimensional barcode.

4. The apparatus of claim 1 wherein the representation includes at least one data matrix symbol.

20 5. The apparatus of claim 1 wherein the second data element concerns a postage value, and the first data element concerns a descending register value.

25 6. The apparatus of claim 1 wherein the representation includes a bit map for a print image of at least one coded symbol representing the plurality of data elements.

7. Apparatus for processing a plurality of postal data elements, the apparatus comprising:

a processor for arranging the plurality of postal data elements in an order such that each postal

data element preceding a second postal data element is independent of the second postal data element; and
an output for providing a representation representing the plurality of postal data elements in the
5 arranged order.

8. The apparatus of claim 7 wherein the representation includes at least one barcode.

9. The apparatus of claim 8 wherein the barcode is a 2-dimensional barcode.

10 10. The apparatus of claim 7 wherein the representation includes at least one data matrix symbol.

11. The apparatus of claim 7 wherein one of the plurality of the data elements concerns a postage value.

15 12. The apparatus of claim 7 wherein the representation includes a bit map for a print image of at least one coded symbol representing the plurality of postal data elements.

20 13. Apparatus for conducting a postage franking transaction to generate a representation representing data, the apparatus comprising:

a processor for identifying a first subset of the data which is unaffected by the postage franking transaction and a second subset of the data which is
25 subject to change during the postage franking transaction; and

an output for providing a representation representing the first subset of the data and the second subset of the data, the representation being partitioned
30 into a first part and a second part thereof, the first subset of the data and the second subset of the data

-25-

being represented by the first part and the second part, respectively.

14. The apparatus of claim 13 wherein the representation includes at least one coded symbol.

5 15. The apparatus of claim 14 wherein the coded symbol includes a barcode.

16. The apparatus of claim 15 wherein the barcode is a 2-dimensional barcode.

10 17. The apparatus of claim 14 wherein the coded symbol includes a data matrix symbol.

18. The apparatus of claim 13 wherein the representation includes a first coded symbol and a second coded symbol, the first part including at least part of the first coded symbol.

15 19. The apparatus of claim 18 wherein the second part includes at least part of the second coded symbol.

20 20. Apparatus for conducting postage franking transaction, the apparatus comprising:

20 a processor for processing a plurality of data elements; and

25 an output for generating at least a first symbol and a second symbol representing the data elements, at least part of the first symbol representing a first subset of the data elements which is unaffected by the postage franking transaction, and at least part of the second symbol representing a second subset of the data elements which is subject to change during the postage franking transaction.

-26-

21. The apparatus of claim 20 wherein the first symbol is generated before the second symbol.

22. The apparatus of claim 20 wherein at least one of the first and second symbols includes a barcode.

5 23. The apparatus of claim 22 wherein the barcode is a 2-dimensional barcode.

24. The apparatus of claim 20 wherein at least one of the first and second symbols includes a data matrix symbol.

10 25. The apparatus of claim 20 wherein the output includes a printer.

26. Apparatus for generating a postage indicium based on at least first data, the first data being a function of second data, the apparatus
15 comprising:

 a processor for determining at least one candidate for the first data based on a predicted version of the second data;

20 a comparator for comparing an actual version of the second data with the predicted version thereof; and

 an output for generating the postage indicium based on the candidate for the first data when the actual version matches the predicted version.

25 27. The apparatus of claim 26 wherein the second data concerns a postage value.

28. The apparatus of claim 27 wherein the second data also concerns a mail class.

-27-

29. The apparatus of claim 26 wherein the predicted version of the second data is statistically determined.

5 30. The apparatus of claim 26 wherein the predicted version of the second data includes a postage value indicated in the last postage indicium generated by the apparatus.

10 31. The apparatus of claim 26 wherein the first data concerns a code for authenticating the postage indicium.

32. The apparatus of claim 31 wherein the code includes at least part of a digital signature.

15 33. The apparatus of claim 26 wherein the processor includes the comparator.

34. Apparatus for creating a postage indicium representing a plurality of data elements, and at least one code for authenticating selected ones of the data elements, the apparatus comprising:
20 an interface for receiving a request for creating the postage indicium; and
a processor for performing computations to generate the code, selected ones of the computations being performed before the request is received, the code
25 being generated based on results of the selected computations after the request is received.

35. The apparatus of claim 34 wherein the code includes a digital signature.

30 36. The apparatus of claim 35 wherein the selected computations include generation of a random number.

-28-

37. The apparatus of claim 36 wherein the selected computations include a computation based on a value of the random number.

5 38. The apparatus of claim 35 wherein the selected computations include a computation of a signature value r in accordance with a digital signature algorithm (DSA).

10 39. The apparatus of claim 35 wherein the selected computations include a computation based on a value of a private key in accordance with a cryptographic algorithm.

15 40. Apparatus for printing a symbol representing data, the data being disposed in at least a first segment and a second segment in the symbol, the first segment being separated from the second segment by a delimiter, the apparatus comprising:

20 at least a first printhead and a second printhead for printing the first and second segments, respectively, the first printhead being separated from the second printhead by a gap, the size of the gap being a function of the size of the delimiter.

41. The apparatus of claim 40 wherein the symbol includes a data matrix symbol.

25 42. The apparatus of claim 41 wherein the data matrix symbol is formatted in a dark on light format.

43. The apparatus of claim 41 wherein the data matrix symbol is formatted in a light on dark format.

30 44. The apparatus of claim 41 wherein the data matrix symbol includes finder patterns, and the delimiter forms part of the finder patterns.

-29-

45. The apparatus of claim 40 wherein the symbol includes a barcode.

46. A method for processing a plurality of postal data elements, a first one of the plurality of postal data elements being a function of at least a second one of the plurality of postal data elements, the method comprising:

arranging the plurality of postal data elements in an order where the second postal data element precedes the first postal data element; and

providing a representation representing the plurality of postal data elements in the arranged order.

47. The method of claim 46 wherein the representation includes at least one barcode.

48. The method of claim 47 wherein the barcode is a 2-dimensional barcode.

49. The method of claim 46 wherein the representation includes at least one data matrix symbol.

50. The method of claim 46 wherein the second data element concerns a postage value, and the first data element concerns a descending register value.

51. The method of claim 46 wherein the representation includes a bit map for a print image of at least one coded symbol representing the plurality of data elements.

52. A method for processing a plurality of postal data elements, the method comprising:

arranging the plurality of postal data elements in an order such that each postal data element preceding

a second postal data element is independent of the second postal data element; and

providing a representation representing the plurality of postal data elements in the arranged order.

5 53. The method of claim 52 wherein the representation includes at least one barcode.

54. The method of claim 53 wherein the barcode is a 2-dimensional barcode.

10 55. The method of claim 52 wherein the representation includes at least one data matrix symbol.

56. The method of claim 52 wherein one of the plurality of the data elements concerns a postage value.

15 57. The method of claim 52 wherein the representation includes a bit map for a print image of at least one coded symbol representing the plurality of postal data elements.

58. A method for conducting a postage franking transaction to generate a representation representing data, the method comprising:

20 identifying a first subset of the data which is unaffected by the postage franking transaction and a second subset of the data which is subject to change during the postage franking transaction; and

25 providing a representation representing the first subset of the data and the second subset of the data, the representation being partitioned into a first part and a second part thereof, the first subset of the data and the second subset of the data being represented by the first part and the second part, respectively.

-31-

59. The method of claim 58 wherein the representation includes at least one coded symbol.

60. The method of claim 59 wherein the coded symbol includes a barcode.

5 61. The method of claim 60 wherein the barcode is a 2-dimensional barcode.

62. The method of claim 59 wherein the coded symbol includes a data matrix symbol.

10 63. The method of claim 58 wherein the representation includes a first coded symbol and a second coded symbol, the first part including at least part of the first coded symbol.

64. The method of claim 63 wherein the second part includes at least part of the second coded symbol.

15 65. A method for conducting postage franking transaction, the method comprising:
 processing a plurality of data elements; and
 generating at least a first symbol and a second
20 symbol representing the data elements, at least part of the first symbol representing a first subset of the data elements which is unaffected by the postage franking transaction, and at least part of the second symbol
 representing a second subset of the data elements which
25 is subject to change during the postage franking transaction.

66. The method of claim 65 wherein the first symbol is generated before the second symbol.

67. The method of claim 65 wherein at least one of the first and second symbols includes a barcode.

-32-

68. The method of claim 67 wherein the barcode is a 2-dimensional barcode.

69. The method of claim 65 wherein at least one of the first and second symbols includes a data
5 matrix symbol.

70. A method for generating a postage indicium based on at least first data, the first data being a function of second data, the method comprising:
determining at least one candidate for the
10 first data based on a predicted version of the second data;
comparing an actual version of the second data with the predicted version thereof; and
generating the postage indicium based on the
15 candidate for the first data when the actual version matches the predicted version.

71. The method of claim 70 wherein the second data concerns a postage value.

72. The method of claim 71 wherein the second
20 data also concerns a mail class.

73. The method of claim 70 wherein the predicted version of the second data is statistically determined.

74. The method of claim 70 wherein the
25 predicted version of the second data includes a postage value indicated in the last postage indicium generated by the method.

75. The method of claim 70 wherein the first data concerns a code for authenticating the postage
30 indicium.

76. The method of claim 75 wherein the code includes at least part of a digital signature.

77. A method for creating a postage indicium representing a plurality of data elements, and at least
5 one code for authenticating selected ones of the data elements, the method comprising:

performing computations to generate the code, wherein selected ones of the computations being performed before a request for creating the postage indicium is
10 received;

receiving the request; and
generating the code based on results of the selected computations after the request is received.

78. The method of claim 77 wherein the code
15 includes a digital signature.

79. The method of claim 78 wherein the selected computations include generation of a random number.

80. The method of claim 79 wherein the
20 selected computations include a computation based on a value of the random number.

81. The method of claim 78 wherein the selected computations include a computation of a signature value r in accordance with a DSA.

82. The apparatus of claim 78 wherein the
25 selected computations include a computation based on a value of a private key in accordance with a cryptographic algorithm.

83. A method for use in an apparatus for
30 printing a symbol representing data, the data being

-34-

disposed in at least a first segment and a second segment in the symbol, the first segment being separated from the second segment by a delimiter, the apparatus including at least a first printhead and a second printhead, the

5 method comprising:

separating the first printhead from the second printhead by a gap, the size of the gap being a function of the size of the delimiter; and

10 printing the first and second segments using the first and second printheads, respectively.

84. The method of claim 83 wherein the symbol includes a data matrix symbol.

85. The method of claim 84 wherein the data matrix symbol is formatted in a dark on light format.

15 86. The method of claim 84 wherein the data matrix symbol is formatted in a light on dark format.

87. The method of claim 84 wherein the data matrix symbol includes finder patterns, and the delimiter forms part of the finder patterns.

20 88. The method of claim 83 wherein the symbol includes a barcode.

1/7

FIG. 1A

PRIOR ART

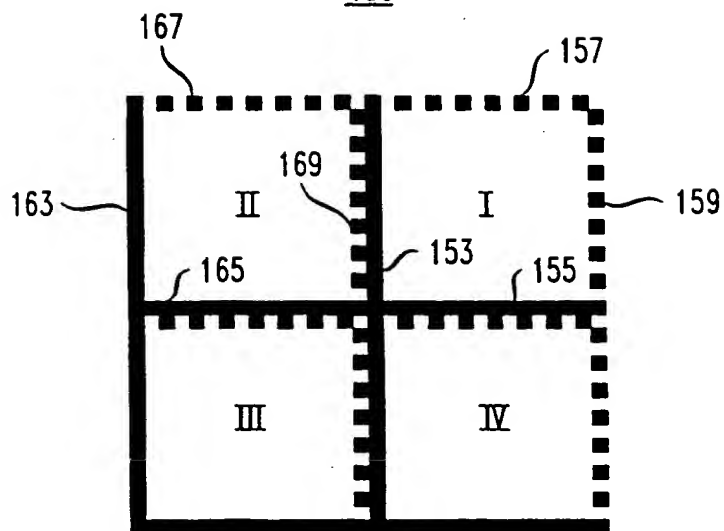
100



FIG. 1B

PRIOR ART

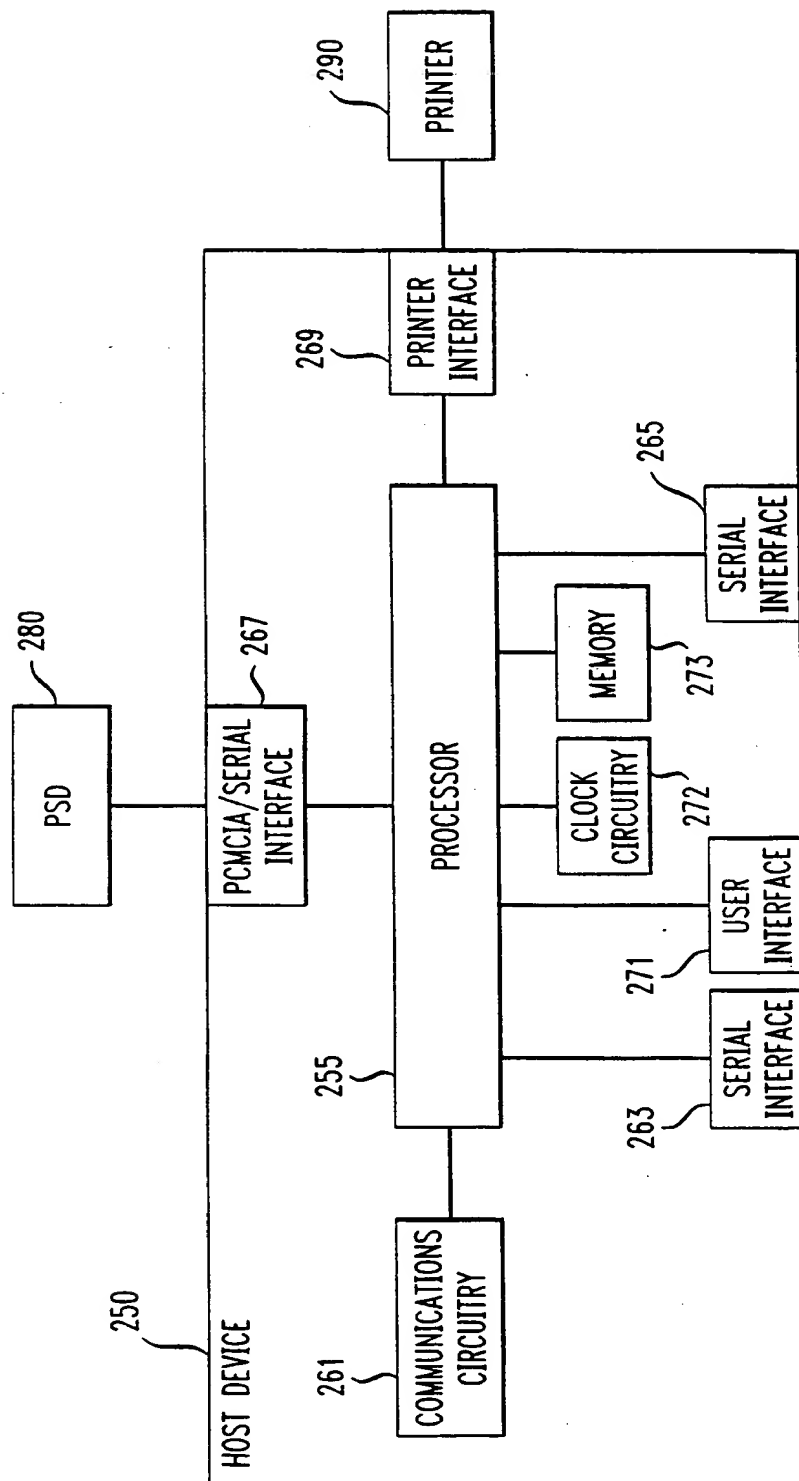
150



THIS PAGE BLANK (USPTO)

2/7

FIG. 2
201



THIS PAGE BLANK (USPTO)

3/7

FIG. 3

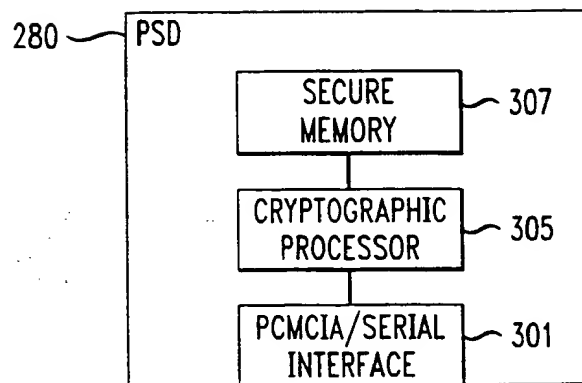
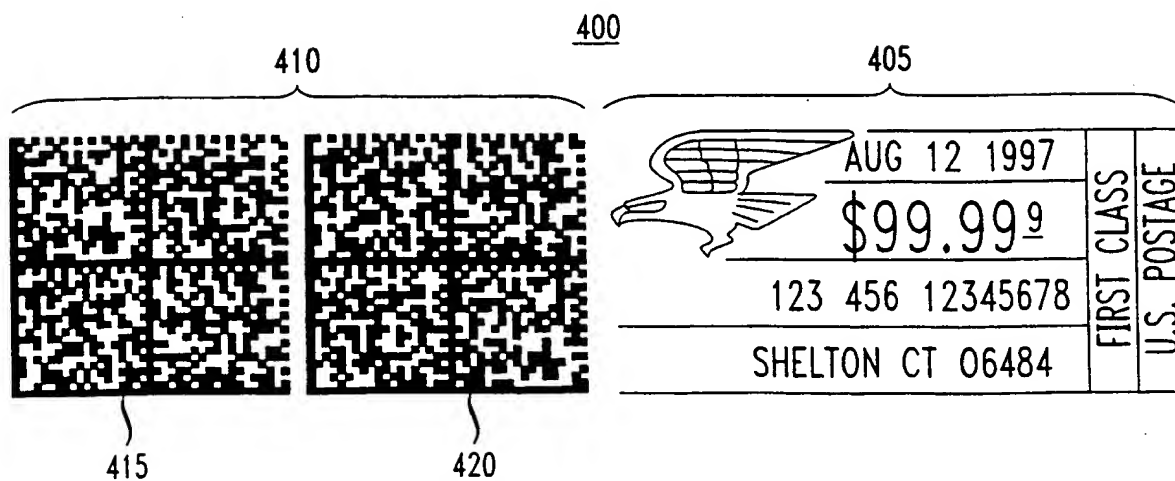


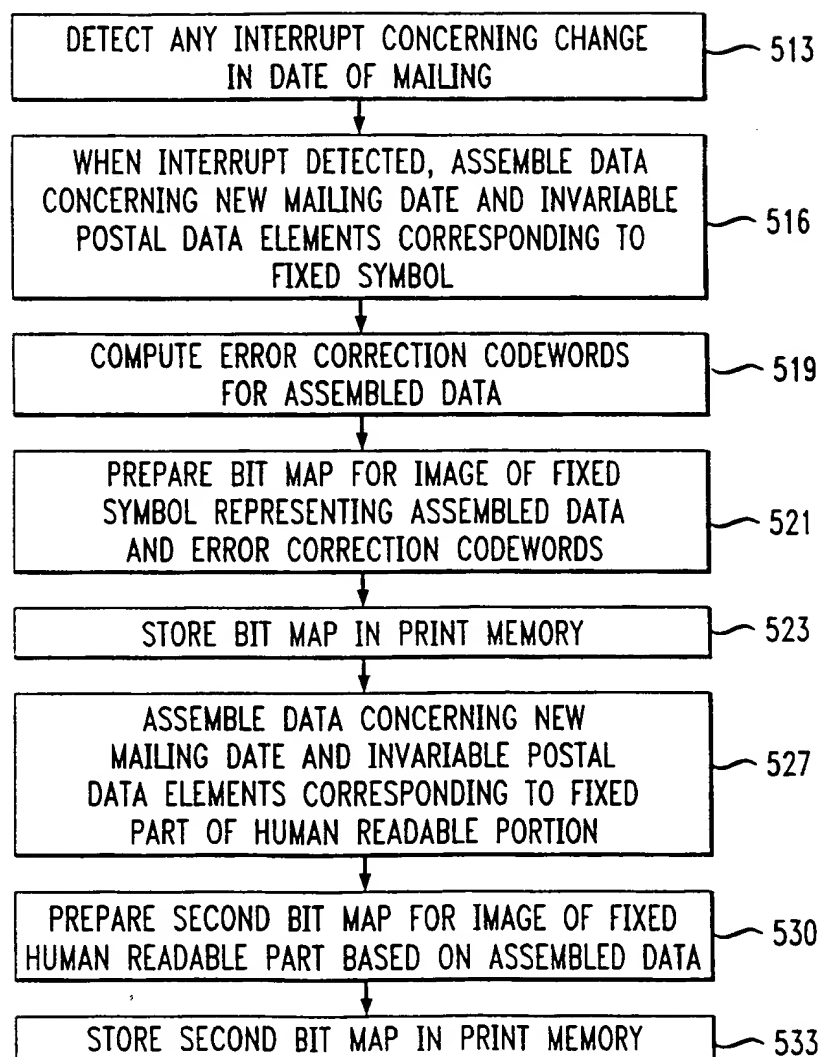
FIG. 4



THIS PAGE BLANK (USPTO)

4/7

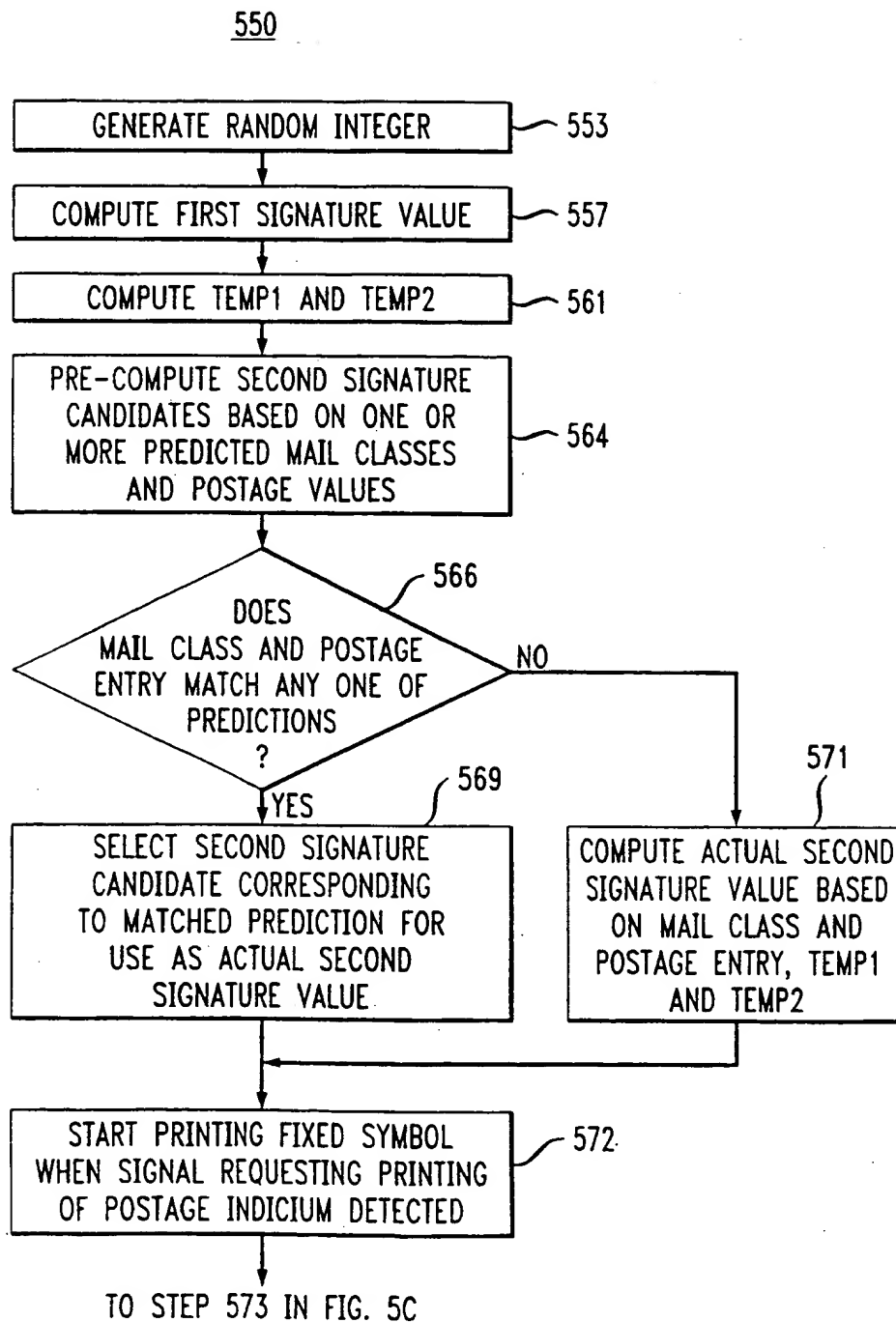
FIG. 5A

503

THIS PAGE BLANK (USPTO)

5/7

FIG. 5B



THIS PAGE BLANK (USPTO)

6/7

FIG. 5C

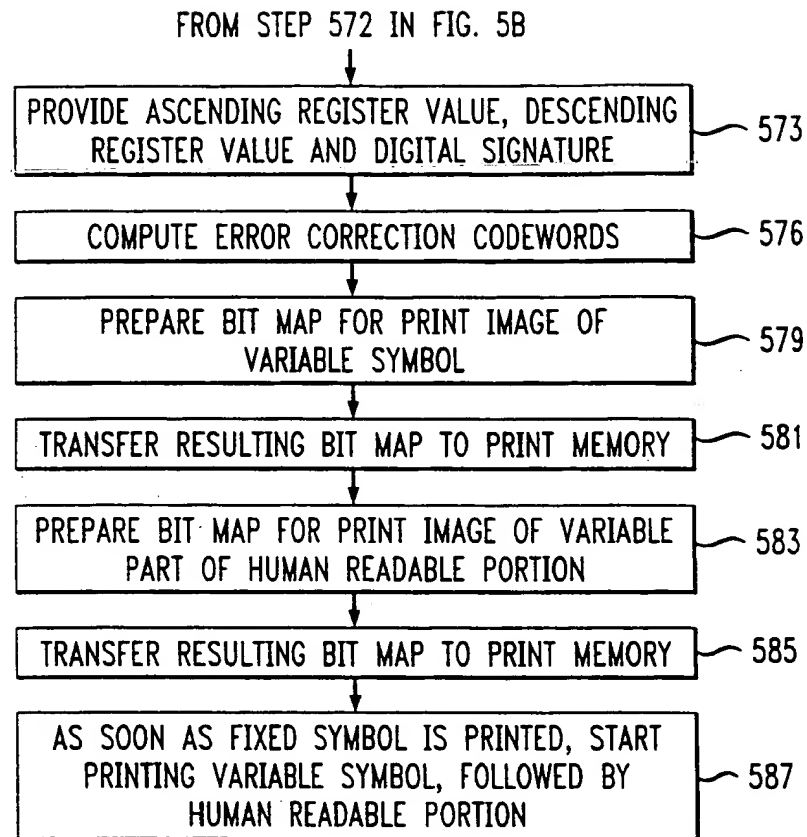
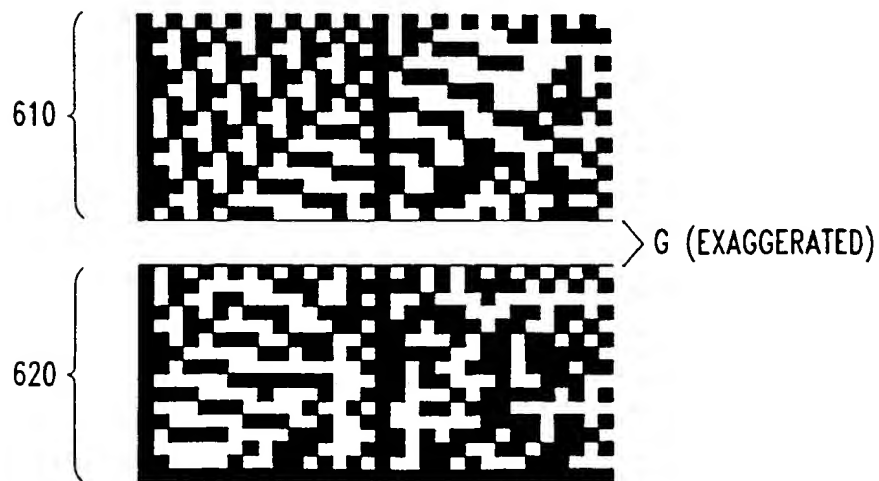


FIG. 6

600

SUBSTITUTE SHEET (RULE 26)

THIS PAGE BLANK (USPTO)

7/7

FIG. 7

700

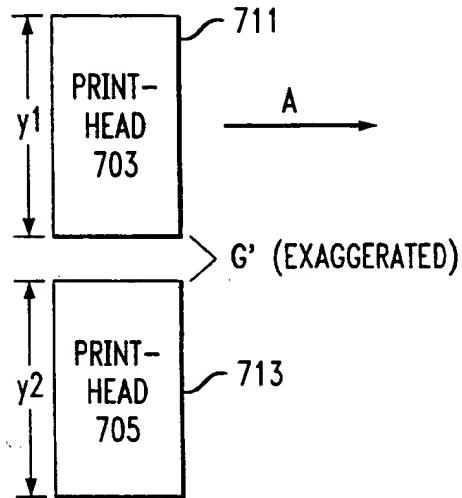
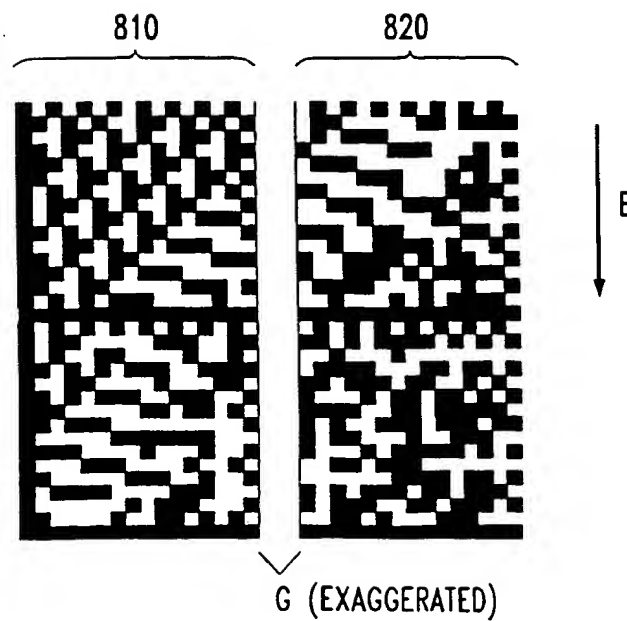


FIG. 8

800



THIS PAGE BLANK (USPTO)